(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11340968 A

(43) Date of publication of application: 10.12.99

(51) Int. Cl H04L 9/32
G09C 1/00
G09C 1/00

(21) Application number: 10145284

(22) Date of filing: 27.05.98

(71) Applicant: MITSUBISHI ELECTRIC CORP

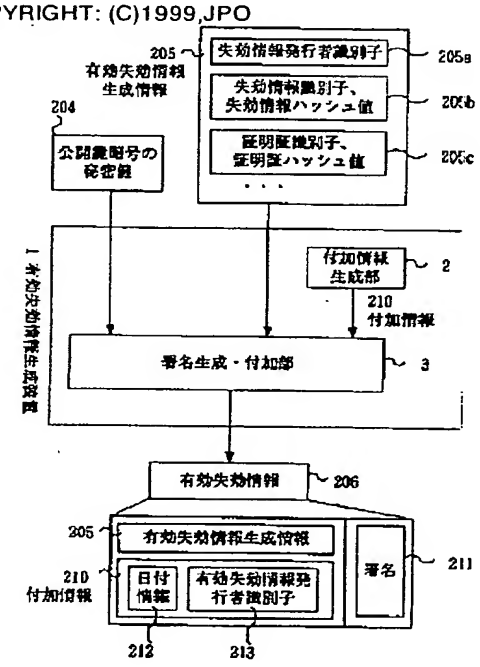
(72) Inventor: SAKAKIBARA HIROYUKI
YOSHITAKE ATSUSHI

(54) INVALID INFORMATION VERIFICATION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To reduce processing to verify the information denoting that a certificate is invalid.

SOLUTION: The system is provided with an additional information generating section 2 that generates additional information 210 consisting of date information 212 denoting the validity of valid-invalid information 206 for verifying the information, a valid-invalid information issuing party identifier 213, a signature generating addition section 3 that receives one set of combinations of an identifier 205a of an invalid information issuing party. A set or more of an identifier 205b of invalid information, an invalid information hash value 205b, an identifier 205c for a certificate for verifying the information to verify a signature of the invalid information, and a hash value 205c for the invalid information verification certificate are inputted. These input data with the additional information 210 generated by the additional information generating section 2 are merged, a signature 211 by a secret key 204 of a public key encryption held by a management agent for the invalid information is added to the merged data. The system is also provided with a signature generating and adding part 3 for the valid invalid information.



(19) 日本国特許庁 (JP)

(12) 公開特許公報（A）

(11) 特許出願公開番号

特開平１１－３４０９６８

(43) 公開日 平成 11 年 (1999)12 月 10 日

(51)Int.Cl.[6]		識別記号	F.I		
H04L	9/32		H04L	9/00	675 B
G09C	1/00	620	G09C	1/00	620 Z
		640			640 B
					640 Z
			H04L	9/00	675 D

審査請求 未請求 請求項の数 9 OL （全 11 頁）

(21) 出願番号 特願平10-145284

(22) 出願日 平成 10 年 (1998)5 月 27 日

(71) 出願人 000006013
三菱電機株式会社
東京都千代田区丸の内二丁目2番3号

(72) 発明者 榊原 裕之
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72) 発明者 吉武 淳
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

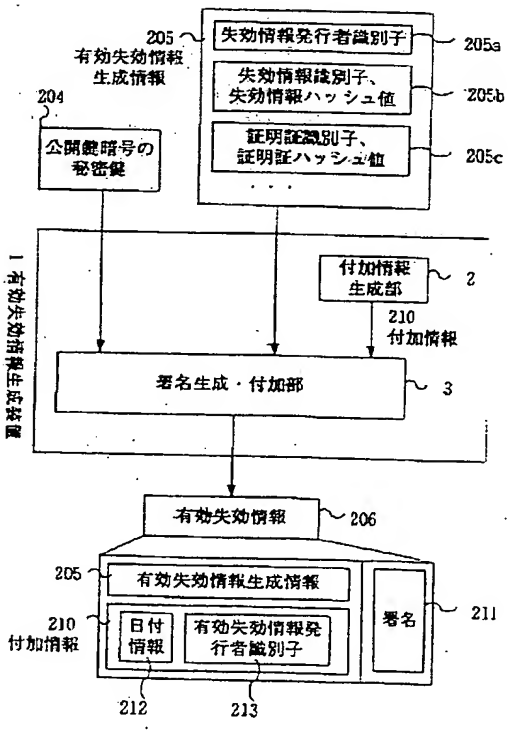
(74) 代理人 弁理士 宮田 金雄 (外2名)

(54)【発明の名称】失効情報検証方式

(57)【要約】

【課題】 証明証が失効したことを示す失効情報を検証する処理を短縮することを目的とする。

【解決手段】 失効情報検証用の有効失効情報２０６の有効期限を示す日付情報２１２及び有効失効情報発行者識別子２１３で構成される付加情報２１０を生成する付加情報生成部２を備え、失効情報発行者の識別子２０５ａと、失効情報の識別子２０５ｂと、失効情報ハッシュ値２０５ｂと、失効情報の署名を検証するための失効情報検証用証明証の識別子２０５ｃと、失効情報検証用証明証のハッシュ値２０５ｃとを連結した組みを１つ以上入力し、この入力データと付加情報生成部２により生成された付加情報２１０とを連結し、失効情報の管理機関が保持する公開鍵暗号の秘密鍵２０４による署名２１１を付加し、有効失効情報として生成する署名生成・付加部３をさらに備えた。



【特許請求の範囲】

【請求項１】　以下の手段を備えた失効情報検証方式。

（ａ）認証局により発行された証明証が失効したことを示す失効情報を検証するための有効失効情報の有効期限を示す日付情報と、上記有効失効情報の発行者を示す有効失効情報発行者識別子と、で構成される付加情報を生成する付加情報生成手段；

（ｂ）上記失効情報を発行した者の識別子と、上記失効情報の識別子と、上記失効情報を一方向性ハッシュ関数に入力して得た出力である失効情報ハッシュ値と、上記失効情報の署名を検証するための失効情報検証用証明証の識別子と、この失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力である証明証ハッシュ値とを連結した組みを１つ以上入力し、この入力データと上記付加情報生成手段により生成された付加情報とを連結し、上記失効情報の管理機関が保持する公開鍵暗号の秘密鍵による署名を付加し、上記有効失効情報として生成する署名生成・付加手段。

【請求項２】　以下の手段を備えたことを特徴とする請求項１記載の失効情報検証方式。

（ａ）上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

（ｂ）上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

（ｃ）上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報識別子を用いて該当する失効情報を取得する失効関連情報取得手段；

（ｄ）上記失効関連情報取得手段により取得した失効情報と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報取得時に用いた失効情報識別子を含む組の失効情報ハッシュ値とを比較し、この入力した失効情報の有効性を検証する有効性検証手段。

【請求項３】　上記失効関連情報取得手段は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報識別子を用いて該当する各失効情報を取得することを特徴とする請求項２記載の失効情報検証方式。

【請求項４】　上記失効関連情報取得手段は、上記失効情報識別子を入力し、この入力した識別子を用いて該当する失効情報を取得することを特徴とする請求項２記載の失効情報検証方式。

【請求項５】　上記失効関連情報取得手段は、上記該当する失効情報を取得せずに、取得済みの失効情報を用いることを特徴とする請求項２記載の失効情報検証方式。

【請求項６】　以下の手段を備えたことを特徴とする請求項１記載の失効情報検証方式。

（ａ）上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

（ｂ）上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

（ｃ）上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する失効情報検証用証明証を取得する失効関連情報取得手段；

（ｄ）上記失効関連情報取得手段により取得した失効情報検証用証明証と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報検証用証明証取得時に用いた失効情報検証用証明証の識別子を含む組の証明証ハッシュ値とを比較し、この入力した失効情報検証用証明証の有効性を検証する有効性検証手段。

【請求項７】　上記失効関連情報取得手段は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する各失効情報検証用証明証を取得することを特徴とする請求項６記載の失効情報検証方式。

【請求項８】　上記失効関連情報取得手段は、上記失効情報検証用証明証の識別子を入力し、この入力した識別子を用いて該当する失効情報検証用証明証を取得することを特徴とする請求項６記載の失効情報検証方式。

【請求項９】　上記失効関連情報取得手段は、上記該当する失効情報検証用証明証を取得せずに、取得済みの失効情報検証用証明証を用いることを特徴とする請求項６記載の失効情報検証方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、公開鍵暗号システムにおける公開鍵証明証の検証において、公開鍵証明証の失効情報を検証する方式に関するものである。

【０００２】

【従来の技術】近年インターネット上での通信において、公開鍵暗号システムの利用が益々要求されている。公開鍵暗号システムを利用した安全な通信においては、認証局が発行した公開鍵証明証が必要となる。公開鍵証明証は、認証局が公開鍵とその持ち主の結びつきを認証局の公開鍵暗号の秘密鍵でデジタル署名を付加して証明したものである。公開鍵を安全に取得するために、公開

鍵は証明証パスと共に検証された公開鍵証明証から取得するべきである。証明証パスはある認証局により署名されたエンティティの証明証と、０個またはそれ以上の数の、別の認証局が発行した証明局の証明証から構成される。加えて、証明証パス上の証明証は失効してないことをチエックされなくてはならないので、認証局が発行する証明証で、有効期限が切れる前に失効したものをリストにしたＣＲＬを失効のチエックに利用することは有効な手法である。

【０００３】公開鍵証明証（以下、証明証という）の検証においては、認証局の証明証の発行形態と失効管理が検証の複雑さを左右する。証明証の発行、検証の方式としては、Network Working Group RFC1422 Privacy Enhancement for Internet Electronic Mail:Part 2: Certificate-Based KeyManagement,February 1993（文献１）や、Federal Public Key Infrastructure(PKI) X.509 Certificate and CRL Extension Profile,NIST PKI-TWG March 9,1998（文献２）に記載のX.509証明証の検証方式等が存在する。これらの方式では、X.509 ver1, ver3ベースの証明証における検証方法を述べている。

【０００４】図４は、認証局の階層構造と証明証の発行形態を示す図であり、RFC1422（文献１）に示された証明証の発行方式を参考にした一例である。認証局（CA1）５０１、認証局（CA2）５０２、認証局（CA3）５０３は階層構造をなし、認証局（CA1）５０１は、自己署名証明証である証明証（Cert_CA1）６０１を自分自身で発行し、さらに、認証局（CA2）５０２に証明証（Cert_CA2）６０２を発行する。認証局（CA2）５０２は、認証局（CA3）５０３に証明証（Cert_CA3）６０３を発行し、認証局（CA3）５０３は、UserA５０５に証明証（Cert_UserA）６０４を発行する。なお、RFC1422（文献１）では、認証局（CA1）５０１に相当するIPRA（Internet Policy Registration Authority）は自身には証明証を発行せず自分の公開鍵のみを公開する。

【０００５】次に、この様な、階層的な証明証の発行形態における各証明証の検証方式を説明する。証明証（Cert_CA1）６０１を検証する場合は、認証局（CA1）５０１が自分自身に発行した自己署名証明証であるので、証明証（Cert_CA1）６０１自身で検証可能である。証明証（Cert_CA2）６０２を検証する場合は証明証（Cert_CA1）６０１が必要になり、証明証（Cert_CA3）６０３を検証する場合は証明証（Cert_CA2）６０２が必要になり、証明証（Cert_UserA）６０４を検証する場合は証明証（Cert_CA3）６０３が必要になる。すなわち、この例では、証明証の検証は、信頼している最上位の認証局の証明証以外は上位の証明証が必要となる。証明証（Cert_UserA）６０４を検証する場合は、証明証（Cert_CA3）６０３、証明証（Cert_CA2）６０２、証明証（Cert_CA1）６０１を収集し、段階的に各証明証の正当性を検証しなくてはならない。これらの証明証の一連を証明証パスと呼ぶ。

【０００６】図５は、図４において発行された証明証のパスを示す図であり、図５に示すように、各証明証には検証に必要な上位証明証の識別子が含まれている。例えば、証明証（Cert_UserA）６０４においては、中に含まれるCert_CA3_IDが証明証（Cert_CA3）６０３を指している。標準的な証明証である、X.509 ver3においては、この証明証の識別子の内容として、発行者Issuer、authorityKeyIdentifierが該当する。authorityKeyIdentifierは、上位の証明証に含まれるIssuerと通し番号（SerialNumber）、又は、keyIdentifierという上位の証明証に含まれる公開鍵に割り振られた一意な識別子である。従って、ある証明証を検証しようとした場合、その中を調べ、含まれている検証に必要な証明証の識別子をもとに、上位の証明証を収集し、その上位証明証に含まれる検証に必要な証明証の識別子をもとにさらに上位の証明証を収集するといった段階的な作業を必要とする。この例では、信頼している自己署名証明証である自分自身で検証が可能な最上位の認証局（CA1）５０１の証明証まで辿る必要があった。

【０００７】さらに、各証明証について、上位の証明証に含まれる公開鍵で署名を検証した上で、持ち主、有効期限等の整合性の検証を行い、全ての証明証の整合性が確認できたなら証明証（Cert_UserA）６０４を検証できたものとする。この例では、認証局（CA1）５０１が自身に証明証を発行し、検証者はこれを信頼し、この証明証にたどり着くまでパスを探しているが、自分が信頼している他の証明証まで辿るか、信頼する公開鍵で検証可能な証明証を指定してそこまで辿っても良い。RFC1422（文献１）では最上位の認証局(IPRA)は公開鍵のみを公開する。検証者はこの公開鍵を信頼できる手段で取得し、信頼した上で、一段下のPCA（PolicyCertification Authority）の証明証までのパスを検証する。

【０００８】証明証を上位の証明証を用いて段階的に検証することに加えて、認証局によっては、証明証の失効管理を行っている場合がある。図６は、図４において、各認証局が失効情報を発行していることを示す図であり、図６の例では、認証局がX.509のCertificate Revocation List(CRL)を発行している場合を示している。ＣＲＬは証明証が有効期限がきれる前に何らかの理由で失効したことを示す情報であり、認証局が発行した証明証で失効しているものの識別子をリストとして含み、認証局の公開鍵暗号の署名が付加されている。エンドエンティティであるUserA５０５が自分の証明証である証明証（Cert_UserA）６０４を検証するためには、上述の証明証の段階的な検証に加えてＣＲＬを利用して各証明証の失効をチェックする必要がある。

【０００９】ＣＲＬ(CRL_CA1)６１１は、認証局（CA1）５０１が発行するＣＲＬであり、認証局（CA1）５０１が失効を管理している証明証のチェック用に用いる。こ

の場合は、例えば、認証局（CA2）５０２に発行している証明証（Cert_CA2）６０２及び証明証（Cert_CA2■）６０２ａの失効のチェックに用いる。同様に、ＣＲＬ(CRL_CA2)６１２は、認証局（CA2）５０２が発行するＣＲＬであり、認証局（CA3）５０３に発行している証明証（Cert_CA3）６０３及び証明証（Cert_CA3■）６０３ａの失効のチェックに用いる。ＣＲＬ(CRL_CA3)６１３は、認証局（CA3）５０３が発行するＣＲＬであり、証明証（Cert_UserA）６０４の失効のチェックに用いる。なお、証明証（Cert_CA1■）６０１ａ、証明証（Cert_CA2■）６０２ａ、証明証（Cert_CA3■）６０３ａは、各々、ＣＲＬ(CRL_CA1)６１１、ＣＲＬ(CRL_CA2)６１２、ＣＲＬ(CRL_CA3)６１３の署名の検証に必要な公開鍵を含む証明証である。ＣＲＬは、各認証局が公開しており、UserA５０５は各ＣＲＬを取得する必要がある。

【００１０】

【発明が解決しようとする課題】従来の図４のような環境では、検証する証明証の上位の証明証を収集し、その中に含まれる検証に必要な上位の証明証の識別子を元にさらに上位証明証を収集するということを繰り返し、自己署名証明証にあたるまで収集を繰り返して証明証パスを形成する。そして、収集が終了したならば、収集した証明証を用いて、各証明証間の整合性の検証を行うという処理を行なっていた。又は、検証する証明証の上位の証明証を収集し、２つの証明証間の整合性を検証し、それが成功したならば上位の証明証に含まれる検証に必要な上位の証明証の識別子を元にさらに上位証明証を収集し、２つの整合性を検証するということを繰り返し、自己署名証明証が見つかるまでくりかえすという処理を行なっていた。これらの処理方式によれば、証明証の中の検証に必要な証明証識別子を調べて、上位証明証を収集するという作業は時間がかかるので、総合的にみると検証に時間がかかるという問題点があった。

【００１１】加えて、認証局が失効管理をしている場合は、ＣＲＬ等の失効情報を利用し証明証の失効の確認をする必要があった。ＣＲＬの様に署名が存在する失効情報の検証においては、署名を検証するために認証局の証明証を必要とするが、この証明証に対しても証明証パスが生ずる。図６に示される証明証・ＣＲＬの発行形態において、図７にＣＲＬ(CRL_CA3)６１３の署名を検証するための証明証パスを示す。ＣＲＬ(CRL_CA3)６１３の署名を検証するためには、署名を検証するための公開鍵を含む証明証（Cert_CA3■）６０３ａが必要であり、ＣＲＬ(CRL_CA3)６１３にはこれを示す識別子Cert_CA3■_IDが含まれている。同様にして、証明証（Cert_CA3■）６０３ａを検証するためには、認証局（CA1）５０１が認証局（CA2）５０２に発行した証明証（Cert_CA2■■）６１４が必要であり、証明証（Cert_CA2■■）６１４を検証するためには、認証局（CA1）が自身に発行した自己署名型の証明証である証明証（Cert_CA1■■）６１５が必要となる。

【００１２】このＣＲＬに関する証明証のパスである証明証（Cert_CA3■）６０３ａ、証明証（Cert_CA2■■）６１４、証明証（Cert_CA1■■）６１５と、図５における証明証（Cert_UserA）６０４に関するパスである証明証（Cert_CA3）６０３、証明証（Cert_CA2）６０２、証明証（Cert_CA1）６０１が同じ場合もあり、その場合は、証明証（Cert_CA3■）６０３ａと証明証（Cert_CA3）６０３、証明証（Cert_CA2■■）６１４と証明証（Cert_CA2）６０２、証明証（Cert_CA1■■）６１５と証明証（Cert_CA1）６０１が同一である。この場合は、パスの検証は一度で済む。しかし、認証局の運用によっては、各証明証が同一ではない場合があり、従って各パスが異なるケースが生じる。その場合は各パスについて、別々に署名を含めた検証を行わなくてはならない。図６の様に、複数のＣＲＬが存在する場合に、各ＣＲＬに関する証明証のパスについても同様で、悪い場合、調べなくてはいけないＣＲＬの数分、証明証のパスが付加的に発生する。前述のように、証明証パスの収集、署名、項目の検証自体が時間のかかる処理であることに加え、失効情報の署名を確認するために、付加的な証明証のパスが発生し、本来検証したい証明証のパスの検証処理が大きくなるという問題点があった。

【００１３】この発明は、上記のような問題点を解決するためになされたもので、ある証明証を検証するために発生した証明証パスにおいて、パス上の各証明証の失効状態を確認するのに必要なＣＲＬ等の署名付き失効情報を検証する場合に、この情報に対して発生した証明証のパスの検証を簡略化することで、検証処理全体を短縮することを目的とする。

【００１４】

【課題を解決するための手段】請求項１の失効情報検証方式は、以下の手段を備えたものである。

（ａ）認証局により発行された証明証が失効したことを示す失効情報を検証するための有効失効情報の有効期限を示す日付情報と、上記有効失効情報の発行者を示す有効失効情報発行者識別子と、で構成される付加情報を生成する付加情報生成手段；

（ｂ）上記失効情報を発行した者の識別子と、上記失効情報の識別子と、上記失効情報を一方向性ハッシュ関数に入力して得た出力である失効情報ハッシュ値と、上記失効情報の署名を検証するための失効情報検証用証明証の識別子と、この失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力である証明証ハッシュ値とを連結した組みを１つ以上入力し、この入力データと上記付加情報生成手段により生成された付加情報とを連結し、上記失効情報の管理機関が保持する公開鍵暗号の秘密鍵による署名を付加し、上記有効失効情報として生成する署名生成・付加手段。

【００１５】請求項２の失効情報検証方式は、以下の手

段を備えたものである。

（ａ）上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

（ｂ）上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

（ｃ）上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報識別子を用いて該当する失効情報を取得する失効関連情報取得手段；

（ｄ）上記失効関連情報取得手段により取得した失効情報と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報取得時に用いた失効情報識別子を含む組の失効情報ハッシュ値とを比較し、この入力した失効情報の有効性を検証する有効性検証手段。

【００１６】請求項３の失効情報検証方式は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報識別子を用いて該当する各失効情報を取得する失効関連情報取得手段を備えたものである。

【００１７】請求項４の失効情報検証方式は、上記失効情報識別子を入力し、この入力した識別子を用いて該当する失効情報を取得する失効関連情報取得手段を備えたものである。

【００１８】請求項５の失効情報検証方式は、上記該当する失効情報を取得せずに、取得済みの失効情報を用いる失効関連情報取得手段を備えたものである。

【００１９】請求項６の失効情報検証方式は、以下の手段を備えたものである。

（ａ）上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

（ｂ）上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

（ｃ）上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する失効情報検証用証明証を取得する失効関連情報取得手段；

（ｄ）上記失効関連情報取得手段により取得した失効情報検証用証明証と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報検証用証明証取得時に用いた失効情報検証用証明証の識別子を含む組の証明証ハッシュ値とを比較し、この入力した失効情報検証用証明証の有効性を検証する有効性検証手段。

【００２０】請求項７の失効情報検証方式は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する各失効情報検証用証明証を取得する失効関連情報取得手段を備えたものである。

【００２１】請求項８の失効情報検証方式は、上記失効情報検証用証明証の識別子を入力し、この入力した識別子を用いて該当する失効情報検証用証明証を取得する失効関連情報取得手段を備えたものである。

【００２２】請求項９の失効情報検証方式は、上記該当する失効情報検証用証明証を取得せずに、取得済みの失効情報検証用証明証を用いる失効関連情報取得手段を備えたものである。

【００２３】

【発明の実施の形態】実施の形態１．以下の実施の形態では、証明証を発行する機関である複数の認証局があり、認証局が他の認証局、又はエンドエンティティに証明証を発行しており、加えてその証明証の失効に関する情報を公開鍵暗号の署名付きの失効情報として配布している環境で、ある証明証を検証する場合について説明する。なお、以下の実施の形態では、失効情報の一例として、X.509のＣＲＬを取り扱う。図１は、この実施の形態における有効失効情報生成装置の構成図である。図において、１は失効情報の検証に用いるための有効失効情報を生成する有効失効情報生成装置、２は有効失効情報の有効期限を示す日付情報２１２と、この有効失効情報生成装置１の保有者の識別子である有効失効情報発行者識別子２１３とで構成される付加情報２１０を生成する付加情報生成部、３は付加情報２１０と有効失効情報生成情報２０５とを入力し、これらを連結し、この有効失効情報生成装置１を保有し、失効情報を管理する機関の公開鍵暗号の秘密鍵２０４を用いてこれに対して署名２１１を生成、付加し、有効失効情報２０６を生成した上で本生成装置の外部に出力する署名生成・付加部であり、有効失効情報生成装置１は、付加情報生成部２と署名生成・付加部３とから構成される。

【００２４】有効失効情報生成情報２０５において、２０５ａは失効情報の発行者の識別子である失効情報発行者識別子、２０５ｂは失効情報識別子、及び失効情報を一方向性ハッシュ関数に与えた結果である失効情報ハッシュ値を連結したもの、２０５ｃは失効情報の署名を検証するための公開鍵を含んだ証明証の識別子である証明証識別子、及び証明証を一方向性ハッシュ関数に与えた結果である証明証ハッシュ値を連結したものであり、この有効失効情報生成情報２０５は、失効情報発行者識別子２０５ａ、失効情報識別子及び失効情報ハッシュ値２

０５ｂ、証明証識別子及び証明証ハッシュ値２０５ｃの組み１つ以上で構成される。

【００２５】図２は、この実施の形態における有効失効情報検証装置の構成図である。図において、４は、図１の有効失効情報生成装置１で生成された有効失効情報２０６を検証する有効失効情報検証装置であり、署名検証部５、付加情報検証部６、失効関連情報取得部７、有効性検証部８とにより構成される。２０８は有効失効情報２０６の署名２１１を検証するための公開鍵暗号の公開鍵であり、有効失効情報を管理する機関の公開鍵である。

【００２６】署名検証部５は公開鍵２０８と有効失効情報２０６を入力とし、有効失効情報２０６の署名２１１を検証する。付加情報検証部６は、署名２１１の検証が済んだ有効失効情報２０６に記載されている日付情報２１２と有効失効情報発行者識別子２１３とを検証し、検証済み有効失効情報２２０を出力する。失効関連情報取得部７は、失効情報の発行者の識別子である失効情報発行者識別子２０７と検証済み有効失効情報２２０とを入力し、検証済み有効失効情報２２０に含まれている、失効情報発行者識別子２０７に該当する失効情報識別子２２１を判別する。加えて、失効情報識別子２２１を用いて装置外部から、該当する失効情報２２２を取得し、有効性検証部８に引き渡す。加えて、検証済み有効失効情報２２０に含まれている、失効情報発行者識別子２０７に該当する失効情報２２２の署名を検証するための公開鍵を含んだ証明証を示す識別子である証明証識別子２２３を判別し、これを用いて装置外部から該当する証明証２２４を取得し、有効性検証部８に引き渡す機能も有する。

【００２７】有効性検証部８は、失効情報２２２と検証済み有効失効情報２２０とを入力し、検証済み有効失効情報２２０に含まれている失効情報２２２に該当する失効情報のハッシュ値を取り出し、これと失効情報２２２を一方向性ハッシュ関数に入力した結果であるハッシュ値と比較し、一致を確認する。一致したならば、検証済み失効情報２２５として装置外部に出力し、一致しなかった場合はエラー情報２２７を出力する。加えて、証明証２２４を入力とし検証済み有効失効情報２２０に含まれる、証明証２２４に該当する証明証のハッシュ値を取り出し、証明証２２４のハッシュ値を生成して比較し一致を確認する。一致したならば、検証済み証明証２２６として装置外部に出力し、一致しなかった場合はエラー情報２２７を出力する機能を有する。

【００２８】次に、図６の様に認証局が証明証・ＣＲＬを発行している環境で、図１に示した有効失効情報生成装置１の動作を図３に基づいて説明する。図３は、図１に示した有効失効情報生成装置１と、図２に示した有効失効情報検証装置４との関係を示すと共に、有効失効情報生成装置１による有効失効情報２０６の生成動作を説

明するための図である。図３において、認証局（CA1）１０１は、CA1の識別子CA1_IDと失効情報CRL_CA1をCA1の識別子及び失効情報２０１として失効情報管理機関１０４に渡し、認証局（CA2）１０２は、CA2の識別子CA2_IDと失効情報CRL_CA2をCA2の識別子及び失効情報２０２とし、認証局（CA3）１０３はCA3の識別子CA3_IDと失効情報CRL_CA3をCA3の識別子及び失効情報２０３として、失効情報管理機関１０４に渡す。各失効情報は最新のものを渡すこととする。

【００２９】有効失効情報生成装置１を管理する失効情報管理機関１０４は、識別子及び失効情報２０３におけるCRL_CA3の署名に関して証明証パスを生成する。これは、図７における、証明証（Cert_CA3■）６０３ａ、証明証（Cert_CA2■■）６１４、証明証（Cert_CA1■■）６１５であり、これらに対し失効の検査を含めた必要な検証・検査を全て行い、正当性を検証した上で、証明証（Cert_CA3■）６０３ａに含まれる公開鍵を用いてＣＲＬ(CRL_CA3)６１３の署名を検証する。検証に成功したならば、ＣＲＬ(CRL_CA3)６１３からCRL_CA3の識別子を取り出し、CRL_CA3_IDとする。又、ＣＲＬ(CRL_CA3)６１３を一方向性ハッシュ関数に入力した結果のハッシュ値をh(CRL_CA3)とする。

【００３０】さらに、ＣＲＬ(CRL_CA3)６１３の署名を検証するための公開鍵を含んだ証明証は証明証（Cert_CA3■）６０３ａであるが、証明証（Cert_CA3■）６０３ａの識別子をCert_CA3■から取り出し、Cert_CA3■_IDとする。証明証（Cert_CA3■）６０３ａについても、一方向性ハッシュ関数に入力し、結果のハッシュ値をh(Cert_CA3■)とする。なお、証明証（Cert_CA3■）６０３ａはパスの検証において既に検証済みである。なお、２０５ａ３はCA3_ID、２０５ｂ３はCRL_CA3_IDとh(CRL_CA3)の連結、２０５ｃ３はCert_CA3■_IDとh(Cert_CA3■)の連結である。

【００３１】残りの認証局に関する失効情報も同様の操作を施し、これらを連結して有効失効情報生成情報２０５とする。すなわち、有効失効情報生成情報２０５は、CRL_CA1に関する情報として、失効情報発行者識別子２０５ａをあらわす２０５ａ１と、失効情報識別子及び失効情報ハッシュ値２０５ｂをあらわす２０５ｂ１と、証明証識別子及び証明証ハッシュ値２０５ｃをあらわす２０５ｃ１とを連結し、以下同様に、CRL_CA2に関する情報として、２０５ａ２、２０５ｂ２、２０５ｃ２を連結し、CRL_CA3に関する情報として、２０５ａ３、２０５ｂ３、２０５ｃ３を連結したものである。

【００３２】即ち、図３に示した有効失効情報生成情報２０５の例は、図１に示した有効失効情報生成情報２０５を具体的に示すものであり、CRL_CA1に関する情報は、２０５ａ１=CA1_ID、２０５ｂ１=CRL_CA1_ID.h(CRL_CA1)、２０５ｃ１=Cert_CA1■_ID.h(Cert_CA1■)の連結であり、CRL_CA2に関する情報は、２０５ａ２=CA2_I

D、２０５ｂ２=CRL_CA2_ID,h(CRL_CA2)、２０５ｃ２=Cert_CA2■_ID,h(Cert_CA2■)の連結であり、CRL_CA3に関する情報は、２０５ａ３=CA3_ID、２０５ｂ３=CRL_CA3_ID,h(CRL_CA3)、２０５ｃ３=Cert_CA3■_ID,h(Cert_CA3■)の連結であることを示している。

【００３３】次に、図１に基づいて有効失効情報生成装置１の動作を説明する。有効失効情報生成装置１は、有効失効情報生成情報２０５と、失効情報管理機関１０４の公開鍵暗号の秘密鍵２０４とを入力し、有効失効情報２０６を生成する。有効失効情報２０５と秘密鍵２０４とを有効失効情報生成装置１が入力すると、付加情報生成部２は、有効失効情報２０６の有効期限等を表す日付情報２１２と、有効失効情報発行者識別子２１３とを連結し、付加情報２１０として出力する。署名生成・付加部３は、有効失効情報生成情報２０５と付加情報２１０とを連結した情報に、秘密鍵２０４を利用して署名２１１を付加し、有効失効情報２０６として出力する。即ち、有効失効情報２０６は、有効失効情報生成情報２０５と、日付情報２１２及び有効失効情報発行者識別子２１３から構成される付加情報２１０と、それらに対する署名２１１とから構成される。

【００３４】次に、図６の様に認証局が証明証・ＣＲＬを発行している環境で、図２に示した有効失効情報検証装置４の動作を図３に基づいて説明する。図３において、UserA１０５は証明証の検証者であり、有効失効情報検証装置４を保持している。UserA１０５が自分の証明証（Cert_UserA）６０４を検証する例を挙げる。UserA１０５は証明証（Cert_UserA）６０４を検証するための証明証のパスを図５の様に生成する。すなわち、証明証（Cert_UserA）６０４、証明証（Cert_CA3）６０３、証明証（Cert_CA2）６０２、証明証（Cert_CA1）６０１を収集する。この時点で、証明証に含まれている情報から、失効情報であるＣＲＬの発行者識別子を得ることができる。

【００３５】例として、X.509では、証明証のSubjectが発行者識別子に該当する。すなわち、証明証（Cert_CA3）６０３からはCRL_CA3の発行者であるCA3の識別子CA3_ID、証明証（Cert_CA2）６０２からはCRL_CA2の発行者であるCA2の識別子CA2_ID、証明証（Cert_CA1）６０１からはCRL_CA1の発行者であるCA1の識別子CA1_IDを得る。ここでは、CRL_CA3の有効性を確認するために、有効失効情報２０６と、失効情報発行者識別子２０７としてCA3_ID、失効情報管理機関１０４の公開鍵暗号の公開鍵２０８を有効失効情報検証装置４に入力する。公開鍵２０８については、有効失効情報２０６に含まれる付加情報２１０内の有効失効情報発行者の識別子２１３を調べ、この識別子２１３が示すエンティティが保持する公開鍵を入手する。

【００３６】以降、有効失効情報検証装置４の動作を図２に基づいて説明する。署名検証部５は、有効失効情報

２０６と失効情報管理機関１０４の公開鍵２０８を入力とし、公開鍵２０８を利用して有効失効情報２０６の署名を検証する。署名に関するアルゴリズムは、有効失効情報生成装置１と同じ物を用いることとする。次に、付加情報検証部６は、有効失効情報２０６に含まれる日付情報２１２、有効失効情報の発行者識別子２１３で構成される付加情報２１０を検証し、有効期限などの日付情報が有効であるならば、検証済み有効失効情報２２０として出力する。

【００３７】失効関連情報取得部７は、検証済み有効失効情報２２０を入力とし、さらに、装置外部から、有効性を確認したい失効情報の発行者識別子である失効情報発行者識別子２０７を入力とする。ここでは、認証局（CA3）１０３の発行した失効情報CRL_CA3の有効性を確認するので、CA3_IDを入力する。失効関連情報取得部７では、検証済み有効失効情報２２０に含まれている、有効失効情報生成情報２０５に該当する、CA1_ID, CRL_CA1_ID, h(CRL_CA1), Cert_CA1■_ID, h(Cert_CA1■)と、CA2_ID, CRL_CA2_ID, h(CRL_CA2), Cert_CA2■_ID, h(Cert_CA2■)と、CA3_ID, CRL_CA3_ID, h(CRL_CA3), Cert_CA3■_ID, h(Cert_CA3■)とから、CA3_IDに該当する組を探し、発行している失効情報の識別子であるCRL_CA3_IDを取得する。これを失効情報識別子２２１として利用し、装置外部から該当する失効情報２２２を取得する。この場合は、CRL_CA3が取得される。

【００３８】次に、有効性検証部８は、外部から取得した失効情報２２２であるCRL_CA3と検証済み有効失効情報２２０を入力とし、CRL_CA3を一方向性ハッシュ関数に入力しハッシュ値を計算する。一方向性ハッシュ関数のアルゴリズムは、有効失効情報生成装置１と同じものとする。計算した値をh■(CRL_CA3)とする。有効性検証部８は、CRL_CA3からCRL_CA3_IDを取り出し、これを利用して検証済み有効失効情報２２０に含まれる有効失効情報生成情報２０５に該当する情報からh(CRL_CA3)を取り出し、h■(CRL_CA3)と比較する。一致すれば、検証済み失効情報２２５として出力し、一致しなければ、エラー情報２２７を出力する。取得したCRL_CA3に対して計算したハッシュ値と、署名２１１と付加情報２１０を検証済みの検証済み有効失効情報２２０に含まれるハッシュ値が一致したということは、取得したCRL_CA3は、失効情報管理機関１０４が署名を検証した上で有効失効情報２０６に記載したCRL_CA3の識別子（CRL_CA3_ID）が示すものと一致することを意味する。すなわち、失効情報管理機関１０４が代理で署名の検証を行った失効情報を得たことになる。

【００３９】従って、検証者であるUserA１０５は出力されたCRL_CA1の署名を検証する必要はないので、CRL_CA1の署名に関する証明証のパスも発生しない。ハッシュ値が一致しなかった場合、装置が偽造されたCRL_CA3を取得した可能性があるので、エラーにする。他の失効情

報に関しても同様の操作で、検証済み失効情報として利用することができる。署名の検証に利用する失効情報管理機関の公開鍵は、信頼できる方法で取得したものを利用する。

【００４０】実施の形態２．実施の形態１の有効失効情報検証装置は、検証済み失効情報の出力を行ったが、本実施の形態では、失効情報の署名を検証するための公開鍵を含んだ証明証の有効性を調べる場合について説明する。

【００４１】図２において、検証済み有効失効情報２２０が生成されるまでの動作は実施の形態１に同様である。失効関連情報取得部７は、検証済み有効失効情報２２０を入力とし、加えて装置外部から、取得したい失効情報の発行者識別子である失効情報発行者識別子２０７を入力とする。ここでは、認証局（CA3）１０３の発行した失効情報CRL_CA3を取得するので、CA3_IDを入力とする。失効関連情報取得部７では、検証済み有効失効情報２２０に含まれている、有効失効情報生成情報２０５に該当する、CA1_ID，CRL_CA1_ID，h(CRL_CA1)，Cert_CA1■_ID，h(Cert_CA1■)と、CA2_ID，CRL_CA2_ID，h(CRL_CA2)，Cert_CA2■_ID，h(Cert_CA2■)と、CA3_ID，CRL_CA3_ID，h(CRL_CA3)，Cert_CA3■_ID，h(Cert_CA3■)とから、CA3_IDに該当する組を探し、失効情報を検証するための証明証の識別子であるCert_CA3■_IDを取得する。これを証明証識別子２２３として利用し、装置外部から該当する証明証２２４を取得する。この場合は、Cert_CA3■が取得される。

【００４２】次に、有効性検証部８は、外部から取得した証明証２２４であるCert_CA3■と検証済み有効失効情報２２０を入力とし、Cert_CA3■を一方向性ハッシュ関数に入力しハッシュ値を計算する。一方向性ハッシュ関数のアルゴリズムは、有効失効情報生成装置１と同じものとする。計算した値をh■(Cert_CA3■)とする。有効性検証部８は、Cert_CA3■からCert_CA3■_IDを取り出し、これを利用して検証済み有効失効情報２２０に含まれる有効失効情報生成情報２０５に該当する情報からh(Cert_CA3■)を取り出し、h■(Cert_CA3■)と比較する。一致すれば、検証済み証明証２２６として出力し、一致しなければ、エラー情報２２７を出力する。実施の形態１と同様の理由で、検証済み証明証２２６の署名に関する検証はおこなう必要がないので、この署名に関する証明証のパスは発生しない。又、ハッシュ値が一致しなかった場合、装置が偽造されたCert_CA3■を取得した可能性があるので、エラーにする。UserA１０５は検証済み証明証２２６であるCert_CA3■を用いて、CRL_CA3の署名を検証する必要がある。本実施の形態では、CRL_CA3を既に取得していて、失効情報の署名を検証するための公開鍵を含んだ証明証を取得したい場合に有効である。

【００４３】実施の形態３．実施の形態１の有効失効情報検証装置４においては、失効情報者識別子をCA3_ID１つだけに設定したが、CA3_ID，CA2_ID，CA1_IDを連結して設定した場合は、検証済み有効失効情報２２０を生成した後で、失効関連情報取得部７はCA3_ID,CA2_ID，CA1_IDの順番に従い、失効情報識別子としてCRL_CA3_ID,CRL_CA2_ID,CRL_CA1_IDを用いて、装置外部から失効情報２２２としてCRL_CA3,CRL_CA2，CRL_CA1を取得し、それぞれ、失効情報検証部８に渡し、実施の形態１の様に検証済み有効失効情報２２０に含まれるハッシュ値との比較を行い、検証済み失効情報２２５として出力する。つまり、複数の失効情報の有効性の確認においても、有効失効情報２０６に対して、署名検証部５における署名の検証と、付加情報検証部６における付加情報の検証を1回で済ませることも可能である。

【００４４】実施の形態４．実施の形態２の有効失効情報検証装置４においては、失効情報者識別子をCA3_ID１つだけに設定したが、CA3_ID，CA2_ID，CA1_IDを連結して設定した場合は、検証済み有効失効情報２２０を生成した後で、失効関連情報取得部７はCA3_ID,CA2_ID，CA1_IDの順番に従い、証明証識別子としてCert_CA3■_ID,Cert_CA2■_ID,Cert_CA1■_IDを用いて、装置外部から証明証２２４としてCert_CA3■,Cert_CA2■，Cert_CA1■を取得し、それぞれ、失効情報検証部８に渡し、実施の形態２の様に検証済み有効失効情報２２０に含まれるハッシュ値との比較を行い、検証済み証明証２２６として出力する。つまり、複数の証明証の有効性の確認においても、有効失効情報２０６に対して、署名検証部５における署名の検証と、付加情報検証部６における付加情報の検証を1回で済ませることも可能である。

【００４５】実施の形態５．実施の形態１の有効失効情報検証装置４においては、失効関連情報取得部７に対して、失効情報発行者識別子２０７を入力したが、失効情報識別子２２１が分かっている場合は、失効情報発行者識別子２０７の代わりに失効情報識別子２２１を入力することで、失効情報２２２を取得することも可能である。又、失効情報２２２を既に取得している場合は、失効関連情報取得部７に対してこれらの識別子は入力せず、失効情報２２２を直接入力とし、有効性検証部８に引き渡すことも可能である。

【００４６】実施の形態６．実施の形態２の有効失効情報検証装置４においては、失効関連情報取得部７に対して、失効情報発行者識別子２０７を入力したが、失効情報２２２を検証するための公開鍵を含んだ証明証の識別子が分かっている場合は、失効情報発行者識別子２０７の代わりに証明証識別子２２３を入力することで、該当する証明証２２４を取得することも可能である。又、証明証２２４を既に取得している場合は、失効関連情報取得部７に対してこれらの識別子は入力せず、証明証２２４を直接入力とし、有効性検証部８に引き渡すことも可能である。

【００４７】

【発明の効果】請求項１の発明によれば、証明証が失効したことを示す失効情報を検証するための有効失効情報として、有効失効情報の有効期限を示す日付情報と、上記有効失効情報の発行者を示す有効失効情報発行者識別子と、上記失効情報を発行した者の識別子と、上記失効情報の識別子と、上記失効情報を一方向性ハッシュ関数に入力して得た出力である失効情報ハッシュ値と、上記失効情報の署名を検証するための失効情報検証用証明証の識別子と、この失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力である証明証ハッシュ値と、を含む情報を作成し、上記失効情報の管理機関が保持する公開鍵暗号の秘密鍵による署名を付加するので、失効情報の検証処理を短縮することができる。

【００４８】請求項２の発明によれば、有効失効情報に付加された失効情報管理機関の署名と付加情報とを検証し、その後、失効情報発行者識別子を利用し、有効失効情報で指定される失効情報を取得し、この取得した失効情報のハッシュ値と有効失効情報に含まれるハッシュ値とを比較し、取得した失効情報の有効性を検証することにより、失効情報の署名を直接検証することなく正当性を確認できるので、失効情報の署名検証のための証明証パスが発生せず、失効情報の検証処理を短縮することができる。

【００４９】請求項３の発明によれば、有効性を確認したい失効情報が複数ある場合、有効失効情報検証装置に対してそれら失効情報の発行者識別子を、複数一度に入力した場合でも、有効失効情報の署名を1度検証するだけで、失効情報の識別子で指定される全ての失効情報を取得でき、加えて、それらの署名を直接検証することなく正当性を確認できるという効果がある。

【００５０】請求項４の発明によれば、失効情報識別子が分かっている場合は、失効情報を発行した者の識別子の代わりに、失効情報識別子を入力し、失効情報を取得することにより、検証処理を簡略化することができる。

【００５１】請求項５の発明によれば、失効情報を既に所持している場合は、失効情報を発行した者の識別子や、失効情報識別子を入力することなく、保持している失効情報を用いるので、検証処理をさらに簡略化することができる。

【００５２】請求項６の発明によれば、有効失効情報に付加された失効情報管理機関の署名と付加情報とを検証し、その後、失効情報発行者識別子を利用し、有効失効情報で指定される失効情報検証用証明証を取得し、この取得した失効情報検証用証明証のハッシュ値と有効失効情報に含まれるハッシュ値とを比較し、取得した失効情報検証用証明証の有効性を検証することにより、失効情報検証用証明証の署名を直接検証することなく正当性を確認できるので、失効情報検証用証明証の署名検証のための証明証パスが発生せず、失効情報検証用証明証の検証処理を短縮することができる。

【００５３】請求項７の発明によれば、失効情報の署名を検証するための公開鍵を含んだ証明証が複数あり、有効性を確認したい場合、有効失効情報検証装置に対して、失効情報の発行者の識別子を、複数一度に入力した場合でも、有効失効情報の署名を1度検証するだけで、該当する証明証を全て取得でき、証明証の署名を直接検証することなく正当性を確認できるという効果がある。

【００５４】請求項８の発明によれば、失効情報検証用証明証の識別子が分かっている場合は、失効情報を発行した者の識別子の代わりに、失効情報検証用証明証の識別子を入力し、失効情報検証用証明証を取得することにより、検証処理を簡略化することができる。

【００５５】請求項９の発明によれば、証明証を既に所持している場合は、失効情報を発行した者の識別子や、失効情報検証用証明証の識別子を入力することなく、保持している失効情報検証用証明証を用いるので、検証処理をさらに簡略化することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１における有効失効情報生成装置の構成を示す図である。

【図２】　本発明の実施の形態１における有効失効情報検証装置の構成を示す図である。

【図３】　有効失効情報生成装置及び有効失効情報検証装置の動作を説明するための図である。

【図４】　認証局の階層構造と証明証の発行形態を示す図である。

【図５】　図４において発行された証明証のパスを示す図である。

【図６】　図４において、各認証局が失効情報を発行していることを示す図である。

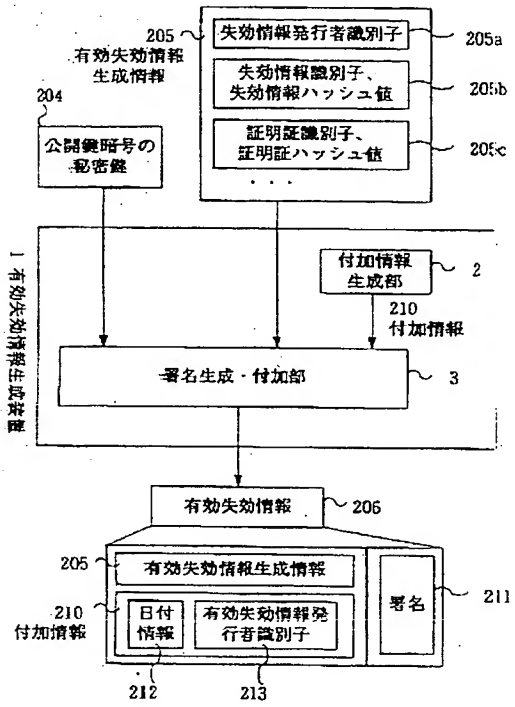
【図７】　署名付きの失効情報に関して証明証パスが存在することを示す図である。

【符号の説明】

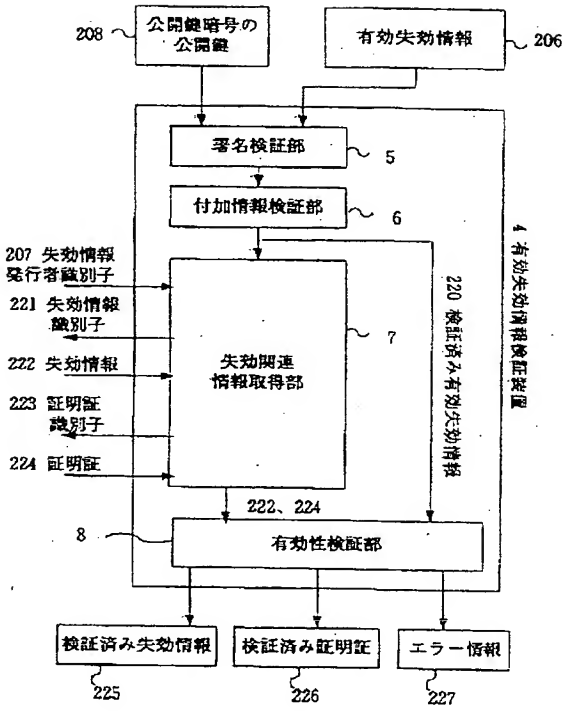
１　有効失効情報生成装置、２　付加情報生成部、３　署名生成・付加部、４有効失効情報検証装置、５　署名検証部、６　付加情報検証部、７　失効関連情報取得部、８　有効性検証部、１０１　認証局（CA1）、１０２　認証局（CA2）、１０３　認証局（CA3）、１０４　失効情報管理機関、１０５　証明証の検証者であるUser A、２０１　CA1の識別子及び失効情報、２０２　CA2の識別子及び失効情報、２０３　CA3の識別子及び失効情報、２０４　秘密鍵、２０５　有効失効情報生成情報、２０５ａ　失効情報発行者識別子、２０５ｂ　失効情報識別子及び失効情報ハッシュ値、２０５ｃ　証明証識別子及び証明証ハッシュ値、２０６　有効失効情報、２０７　失効情報発行者識別子、２０８　公開鍵、２１０　付加情報、２１１　署名、２１２　日付情報、２１３　有効失効情報発行者識別子、２２０　検証済み有効失効情報、２２１　失効情報識別子、２２２　失効情報、２

２３　証明証識別子、２２４　証明証、２２５　検証済み失効情報、２２６　検証済み証明証、２２７　エラー情報。

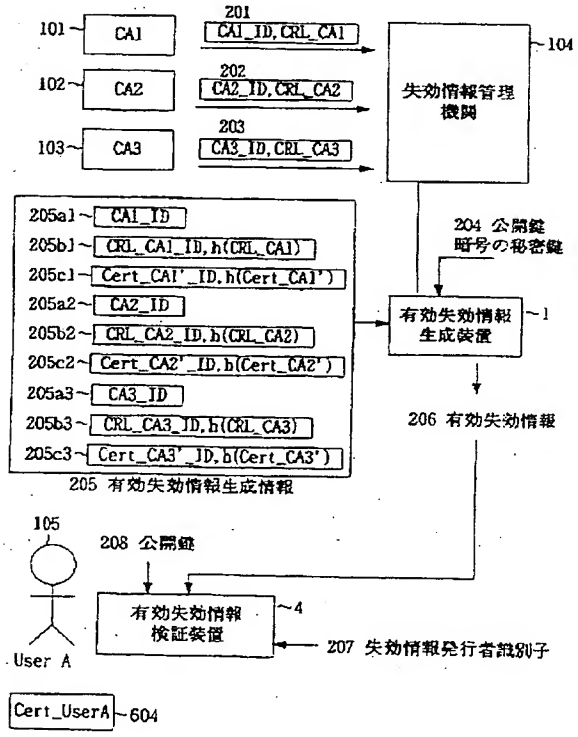
【図１】



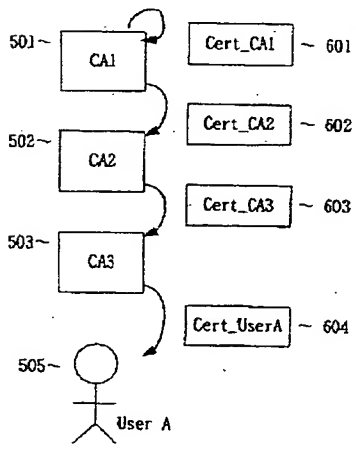
【図２】



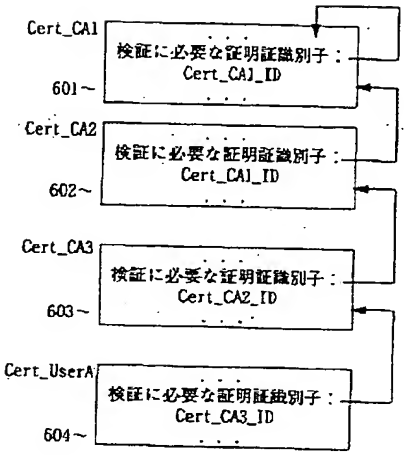
【図３】



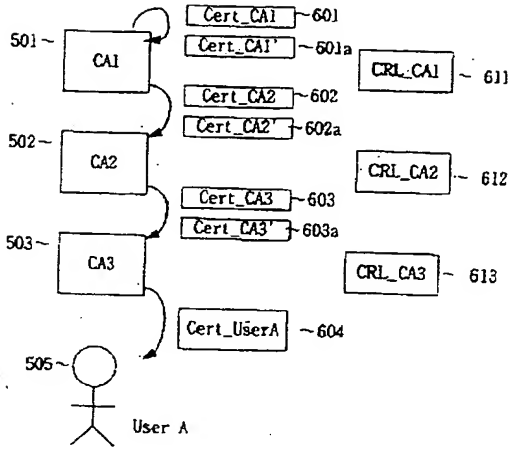
【図４】



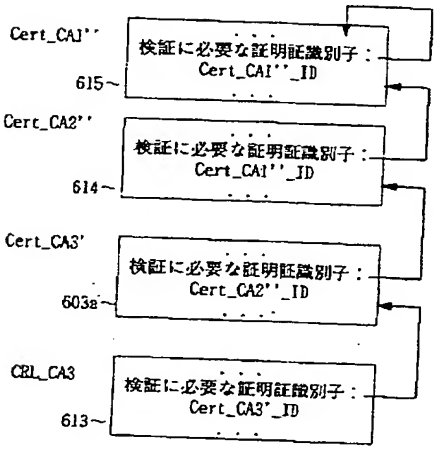
【図５】


Cert_CA1
検証に必要な証明証識別子：
Cert_CA1_ID
601～
Cert_CA2
検証に必要な証明証識別子：
Cert_CA1_ID
602～
Cert_CA3
検証に必要な証明証識別子：
Cert_CA2_ID
603～
Cert_UserA
検証に必要な証明証識別子：
Cert_CA3_ID
604～

【図６】


501～
CA1
Cert_CA1
～601
Cert_CA1'
～601a
CRL_CA1
～ 611
Cert_CA2
～602
Cert_CA2'
～602a
502～
CA2
CRL_CA2
～ 612
Cert_CA3
～603
Cert_CA3'
～603a
503～
CA3
CRL_CA3
～ 613
Cert_UserA
～604
505～
User A

【図７】


Cert_CA1''
検証に必要な証明証識別子：
Cert_CA1''_ID
615～
Cert_CA2''
検証に必要な証明証識別子：
Cert_CA1''_ID
614～
Cert_CA3'
検証に必要な証明証識別子：
Cert_CA2''_ID
603a～
CRL_CA3
検証に必要な証明証識別子：
Cert_CA3'_ID
613～